ThreatQuotient

Team Cymru Controller CDF

Version 1.0.1

February 03, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email:	support@threatq.com
Web:	support.threatq.com
Phone:	703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 4.23
Support Tier	ThreatQ Supported

Introduction

The Team Cymru Controller CDF ingests Indicators with different types, after processing a zipped xml received as a response.

Prerequisites

You will need the following to run the integration:

- A Team Cymru Controller Username.
- A Team Cymru Controller Password.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the file on your local machine

    > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. The feed will now be added to the integrations page. You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

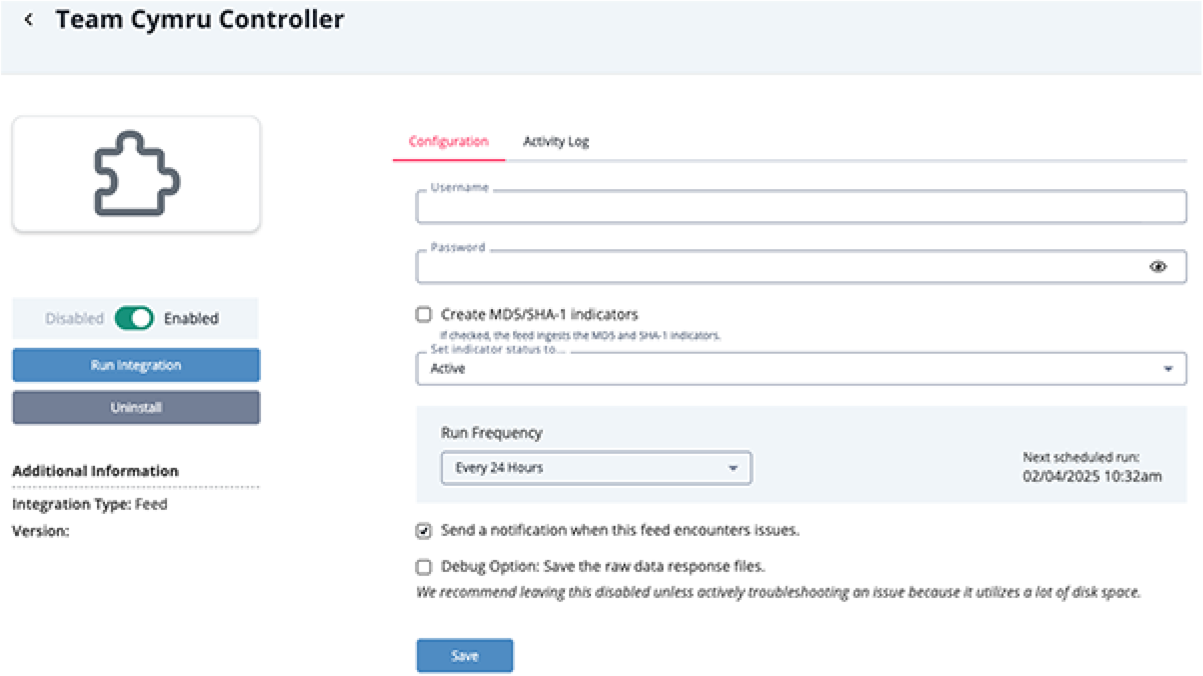
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your Team Cymru Controller username used for authentication.
Password	You Team Cymru Controller password used for authentication.
Create MD5/SHA-1 Indicators	If enabled, the feed will ingest MD5 and SHA-1 indicators. This parameter is not enabled by default.



Username

Password

□ Create MD5/SHA-1 indicators

If checked, the feed ingests the MD5 and SHA-1 indicators.

Set indicator status to...: Active

Run Frequency: Every 24 Hours

Next scheduled run: 02/04/2025 10:32am

☑ Send a notification when this feed encounters issues.

□ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Additional Information

Integration Type: Feed

Version:

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Team Cymru Controller

The main feed used to retrieve indicators data from the Team Cymru Controller endpoint.

```
GET https://downloads.cymru.com/controller_feed/
controllers_{{run_meta.since}}.xml.zip
```

Sample Response:

```
<?xml version="1.0"?>
<botnetlist generated="2020-08-25 14:20:02" version="2.0">
  <botnet resolves="0" proto="6" active="1" first_seen="2019-12-27 17:03:52"
address="188.251.213.180" type="http" id="6E92AA86-E749-382D-BAA3-56D8FCCE9C85"
port="443" family="emotet" subfamily="qbot">
    <http request_type="POST" ssl="0" url="http://188.251.213.180:443/" />
    <controller last_checked="2020-08-25 13:55:44" ip="188.251.213.180"
active="1" came_up="2020-08-22 05:50:11" confidence="60"
first_active="2019-12-27 17:03:52" />
    <malware sha1="2750b83c5eadcf2d3cfa1e3055627157a4ca07d1"
md5="cf418eef4966cedde4b6c4911172bf70" />
    <malware sha1="772f7cd53d6aa898feded856630d72e77721fdc2"
md5="74b975a7426fe9407eb77bcdf63cf81b" />
    ....
  </botnet>
  ....
</botnetlist>
```

ThreatQ provides the following default mapping for this feed, processing only active botnet objects, where active="1":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
botnetlist[].botnet.address	Indicator	FQDN or IP Address	'188.251.213.180'	Processes only active botnet objects, where botnetlist[].botnet.active="1".
botnetlist[].botnet.port	Indicator.Attribute	Port	'443'	
botnetlist[].botnet.family	Indicator.Attribute	Malware Family	'emotet'	
botnetlist[].botnet.subfamily	Indicator.Attribute	Malware Subfamily	'qbot'	
botnetlist[].botnet[].http.url	Related Indicator	URL	'http://188.251.213.180:443/'	
botnetlist[].botnet[].controller.ip	Related Indicator	IP Address	'188.251.213.180'	Processes only active controller objects, where botnetlist[].botnet[].controller.active="1".
botnetlist[].botnet[].controller.confidence	Indicator.Attribute	Confidence	'60'	
botnetlist[].botnet[].malware.sha1	Related Indicator	SHA-1	'2750b83c5eadcf2d3cfa1e3055627157a4ca07d1'	
botnetlist[].botnet[].malware.md5	Related Indicator	MD5	'cf418eef4966cedde4b6c4911172bf70'	

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Team Cymru Controller

METRIC	RESULT
Run Time	3 hours
Indicators	50,148
Indicator Attributes	19,670

Change Log

- **Version 1.0.1**
  - Resolved a `TypeError("'NoneType' object is not iterable")` error that would occur during feed runs.
- **Version 1.0.0**
  - Initial release